

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-023138

(43)Date of publication of application : 22.01.2004

(51)Int.Cl. H04L 9/08  
G06F 12/14  
G06F 12/16  
G06K 17/00

(21)Application number : 2002-171312

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 12.06.2002

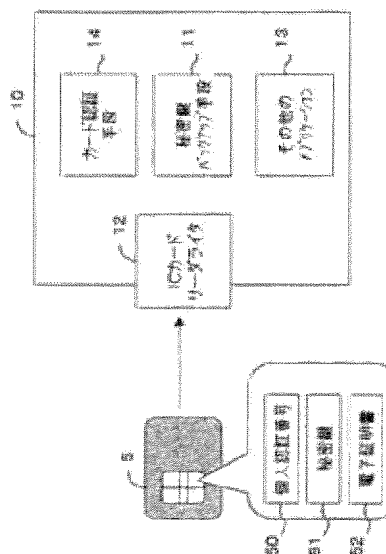
(72)Inventor : ISHIDAIRA IKU

(54) METHOD FOR BACKING UP SECRET KEY AND INFORMATION PROCESSING TERMINAL

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a method for securely restoring a secret key without a cost increase when an IC card is destroyed or missing.

**SOLUTION:** This invention in order to solve the problem provides: the method for backing up the secret key recorded on the IC card characterized in that dividing and encrypting data of the original secret key creates a plurality of divided encryption data and a plurality of other IC cards distributively record the divided encryption data; and an information processing terminal that installs the method on a personal computer.





(19) 日本国特許庁(JP)

(12) 公 開 特 許 公 報(A)

(11) 特許出願公開番号

特開2004-23138

(P2004-23138A)

(43) 公開日 平成16年1月22日(2004.1.22)

(51) Int.Cl.<sup>7</sup>

F I

テーマコード (参考)

H04L 9/00

H04L 9/00

601Z

5B017

G06F 12/14

G06F 12/14

310H

5B018

G06F 12/16

G06F 12/14

320B

5B058

G06K 17/00

G06F 12/16

310M

5J104

G06K 17/00

B

審査請求 未請求 請求項の数 6 O L (全 7 頁)

(21) 出願番号 特願2002-171312(P2002-171312)

(22) 出願日 平成14年6月12日(2002.6.12)

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(74) 代理人 100111659

弁理士 金山 聡

(72) 発明者 石平 郁

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

Fターム(参考) 5B017 AA03 BA07 BA10 CA05 CA14

5B018 GA04 HA04 MA24

5B058 CA01 KA02 KA04 KA08 KA35

YA20

5J104 AA16 EA04 EA20 NA02 NA35

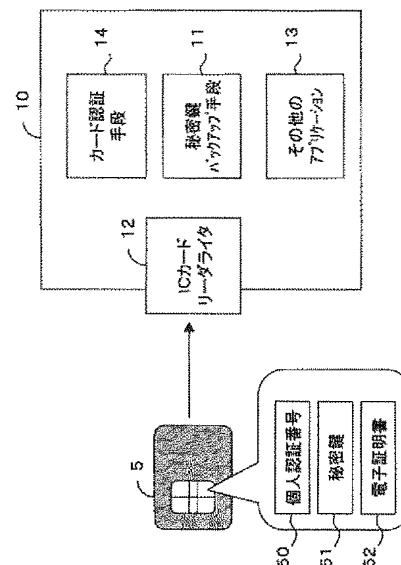
(54) 【発明の名称】 秘密鍵のバックアップ方法および情報処理端末

(57) 【要約】

【課題】 ICカードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧する仕組みを提供することを課題とする。

【解決手段】 ICカードに記録されている秘密鍵のバックアップをとる方法であって、元の秘密鍵のデータを分割して暗号化した複数の分割暗号化データを作成し、他の複数のICカードに前記分割暗号化データを分散して記録させることを特徴とする秘密鍵のバックアップ方法および、この方法をパソコン上に実装した情報処理端末により上記課題を解決する。

【選択図】 図1



## 【特許請求の範囲】

## 【請求項1】

ＩＣカードに記録されている秘密鍵のバックアップをとる方法であって、秘密鍵のデータを分割して暗号化した複数の分割暗号化データを作成し、他の複数のＩＣカードに前記分割暗号化データを分散して記録させることを特徴とする秘密鍵のバックアップ方法。

## 【請求項2】

請求項１に記載の秘密鍵のバックアップ処理方法において、前記分割暗号化データを他の複数のＩＣカードに分散して記録する際、他の複数のＩＣカードの幾つかが失われても元の秘密鍵を復元できるようにするために、前記分散暗号化データを冗長性を持たせて分散して記録することを特徴とする秘密鍵のバックアップ方法。

## 【請求項3】

請求項１または請求項２に記載のバックアップ処理方法における秘密鍵のバックアップ処理、および、バックアップをとった秘密鍵の復旧処理を実行する秘密鍵バックアップ手段を備えた情報処理端末。

## 【請求項4】

請求項３に記載の情報処理端末において、ＩＣカードに記録されている個人認証情報により、そのＩＣカードの所有者が当該情報処理端末を使用できるかどうかを決めるユーザー認証手段を備えており、前記秘密鍵バックアップ手段は、秘密鍵のバックアップを行う際、当該情報処理端末の使用を許可されているユーザーのＩＣカードにのみ、前記分割暗号化データを分散して記録させることを特徴とする情報処理端末。

## 【請求項5】

請求項４に記載の情報処理端末において、前記秘密鍵バックアップ手段は、ＩＣカードから読み出した秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して前記分割暗号化データを作成する機能、および前記分割暗号化データから元の秘密鍵を復元する機能を備えたものである情報処理端末。

## 【請求項6】

請求項１または請求項２に記載のバックアップ処理方法において使用されるＩＣカードであって、分割数を含むバックアップコマンドを受けつけた場合に、秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して前記分割暗号化データを作成して、パソコン側に返答する機能、および復元コマンドとともに一揃いの分割暗号化データを与えられた場合に、元の秘密鍵を復元する機能を備えたＩＣカード。

## 【発明の詳細な説明】

## 【０００１】

## 【発明の属する技術分野】

本発明は、ＩＣカードにより限定した人のみ利用できるパソコン環境内で、ＩＣカードに記録された秘密鍵のバックアップ、および、逸失したＩＣカードに記録されていた秘密鍵の復元に関する。

## 【０００２】

## 【従来技術】

PKI (Public Key Infrastructure : 公開鍵暗号方式によるデジタル署名を用いた電子文書の認証の仕組み) で利用される秘密鍵はＩＣカードに保管される場合がある。秘密鍵は電子環境における、個人の実印を意味する重要なものであり、絶対に漏洩してはならないので、ＩＣカードに保管する場合は、通常、鍵のバックアップはとらない。一方、秘密鍵のバックアップを取る場合は、そのデータが漏洩されないよう機器の設置、運用に関して特別な配慮が必要である。

## 【０００３】

秘密鍵や電子証明書を記録したＩＣカードが破損、紛失した場合は、秘密鍵のバックアップがなければ、これに格納された秘密鍵、電子証明書で署名、暗号化した情報が利用できなくなる。又、秘密鍵のバックアップを取っていると、安全に保管するための機器の設置、運用などが必要で多大な労力をかけている。これを怠るとセキュリティが著しく

低下する。

【0004】

【発明が解決しようとする課題】

P K I の普及が進むことにより、個人の秘密鍵、電子証明書を I C カードに保管して利用する人がますます増えてくるものと予想される。それに伴い、秘密鍵、電子証明書を記録した I C カードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧する仕組みを用意しておく必要がある。

【0005】

本発明はこのような問題点を考慮してなされたものであり、I C カードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧する仕組みを提供することを課題とする。

【0006】

【課題を解決するための手段】

課題を解決するための第1の発明は、

I C カードに記録されている秘密鍵のバックアップをとる方法であって、元の秘密鍵のデータを所定の分割数により分割して暗号化した複数の分割暗号化データを作成し、他の複数の I C カードに前記分割暗号化データを分散して記録させることを特徴とする。

【0007】

第1の発明の方法における望ましい態様は、前記分割暗号化データを他の複数の I C カードに分散して記録する際、他の複数の I C カードの幾つかが失われても元の秘密鍵を復元できるようにするために、前記分散暗号化データを冗長性を持たせて分散して記録することを特徴とする秘密鍵のバックアップ方法である。

【0008】

課題を解決する第2の発明は、第1の発明の方法に係る秘密鍵のバックアップ処理、および、バックアップをとった秘密鍵の復旧処理を実行する秘密鍵バックアップ手段を備えた情報処理端末である。

【0009】

第2の発明の第2の態様は、第2の発明に係る情報処理端末において、I C カードに記録されている個人認証情報により、その I C カードの所有者が当該情報処理端末を使用できるかどうかを決めるユーザー認証手段を備えており、前記秘密鍵バックアップ手段は、秘密鍵のバックアップを行う際、当該情報処理端末の使用を許可されているユーザーの I C カードにのみ、前記分割暗号化データを分散して記録させることを特徴とする情報処理端末である。

【0010】

第2の発明の第3の態様は、第2の発明の第2の態様に係る情報処理端末において、前記秘密鍵バックアップ手段は、I C カードから読み出した秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して前記分割暗号化データを作成する機能、および前記分割暗号化データから元の秘密鍵を復元する機能を備えることを特徴とした情報処理端末である。

【0011】

課題を解決する第3の発明は、第1の発明に係るバックアップ処理方法において使用される I C カードであって、情報処理端末から分割数を含むバックアップコマンドを受けつけた場合に、内部に保持している秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して分割暗号化データを作成して情報処理端末側に返答する機能、および、情報処理端末から復元コマンドとともに一揃いの分割暗号化データを与えられた場合には、元の秘密鍵を復元して内部に保持する機能を備えたことを特徴とするものである。

【0012】

【発明の実施の形態】

以下図面を用いて、本発明の一実施形態である暗号システムを説明してゆく。ここで暗号システムとは P K I を実現する一組の情報処理端末と I C カードを指す。図1は本発明に係る暗号システムの一実施形態である暗号システム1の全体構成を説明するブロック図で

ある。暗号システム1は、秘密鍵バックアップ手段11、カード認証手段14およびその他のアプリケーションプログラム13、ICカードリーダライタ12を備えたコンピュータ10と個人認証番号50および秘密鍵51、電子証明書52を予め記録してあるICカード5とから構成される。尚、コンピュータ10には図示していないが、利用者に対話インターフェースを提供するモニタディスプレイおよびマウス若しくはキーボード等の入力装置が接続されている。以下図面を用いて暗号システム1を説明してゆく。

【0013】

パソコン10はICカードに記録されている個人認証番号より利用者を限定し、利用できないICカード5がリーダライタに挿入された場合は、パソコンを利用させない仕組みを持つものとする。ICカード5がICカードリーダライタ12に挿入されない場合も、利用させない。ICカード5がICカードリーダライタ12に挿入されると、カード認証手段14が自動的に起動され、そのカードの個人認証番号を検査して、上記判定を行う。

【0014】

ICカード5には所有者の個人認証番号50、秘密鍵51および電子証明書52が記録されている。尚、以下の記載および図面において、カードの持ち主AまたはB等を特定してICカード5a、5bなどとも記す。ICカード5というときは持ち主を限定しないでICカードに言及する場合である。他の符号においても同様である。

【0015】

秘密鍵バックアップ手段11は、ICカードリーダライタ12に挿入されているICカード5に記録されている秘密鍵51のバックアップおよび復元処理を行うアプリケーションプログラムである。

【0016】

以下秘密鍵のバックアップを行う場合の手順を説明する。

▲1▼ICカードの個人認証番号によりパソコン10の利用を許可された利用者Aが秘密鍵バックアップ手段11を起動し、秘密鍵51のバックアップを指示する。秘密鍵バックアップ手段11は、秘密鍵51をいくつに分割するかをそのパソコンを利用可能な登録ユーザー数以下で任意に決定する。この分割数は利用者Aが任意に決めてもよい。

▲2▼秘密鍵バックアップ手段11は、ICカード5に対して、秘密鍵51のバックアップコマンドを指令することで、ICカード5から分割、暗号化された秘密鍵を取り出し安全な方法でパソコン内に保管する。例えば分割数を3とした場合は、バックアップコマンドに分割数3をパラメータとして与えてICカードに指令する。ICカード5は、秘密鍵51を3分割し暗号化した秘密鍵分割データ61、62、63を秘密鍵バックアップ手段11に応答する。

▲3▼また、ICカード5の持ち主が新しいICカードに秘密鍵データを復元する時に、持ち主が同一であることを検証するために必要な情報を秘密鍵分割データ61、62、63とともに記録する。例えばICカード5に記録されている個人認証番号を記録する。図2はこの状態を示す。図2において、パソコン10内には、利用者Aの秘密鍵のバックアップのために管理されるデータの集合110が作成され、この中に秘密鍵分割データ61、62、63および利用者Aの個人認証番号50aが記録保持される。

▲4▼次に利用者A以外の人（利用者B）が、この環境を利用するときに、利用者Aの秘密鍵の分割データの1つである61を自動的に利用者BのICカード5bに書きこみ、ICカード5bに書かれた個人認証番号50bを取り出し安全な方法（暗号化など）で記憶しておく。この時、利用者BのICカードに書きこんだ秘密鍵の分割データ61はデータ集合110から消去される。図3はこの状態を示した図である。

▲5▼パソコン10を使用できる他の利用者（利用者C、D）がこの環境を利用するときに、秘密鍵の分割データがなくなるまで上記▲4▼の動作を繰り返す。分割データ60、61、・・・が全て、他のICカードへ書きこまれると、利用者Aの秘密鍵のバックアップは終了となる。パソコン10のデータ集合110には、消去された分割データ60、61、・・・の代わりに、それらが書込まれた先のICカードを特定する個人認証番号50b、50c、50dが残る。図4は、この状態のパソコン10およびデータ集合

110の様子を示している。

【0017】

ICカード紛失時の秘密鍵の復元手順は次の通りである。

▲6▼ICカードを破損、紛失した利用者Aは、新しいICカードを準備し、紛失したICカードの秘密鍵のバックアップをとったパソコン10にて、秘密鍵の復元を指示する。

▲7▼秘密鍵バックアップ手段11が起動する。新しいICカードの持ち主が以前、秘密鍵のバックアップを取った本人であることの認証を行う。これは▲3▼で残したデータ集合110内に記録されている個人認証番号50aが新しいICカードに記録されている個人認証番号50と一致するかどうかで判断する。

▲8▼復元を指示された、秘密鍵バックアップ手段11は、以降、上記▲4▼で記憶したICカードに書かれた固有情報の所有者がこの環境を利用する毎に（これはデータ集合110内に記録されている個人認証番号50b、50c、・・・に一致する個人認証番号をICカード内に含んでいるかによりチェックできる）、以前ICカードに書かれた所有者Aの分割された秘密鍵データ60、61、・・・を取り出し、安全な方法（暗号化されたままの状態）で読み出しデータ集合110に保持する。

▲9▼上記▲3▼で決定した全ての分割秘密鍵データ60、61、63が準備できた段階で、所有者Aの新しいICカードをリーダライタに挿入し、秘密鍵バックアップ手段11を起動させ、組み立て合成を指示するコマンドとともに分割秘密鍵データ60、61、63をICカード5に送り付ける。すると新しいICカードの中で秘密鍵が再構成される。

【0018】

利用者Aの秘密鍵を復元するためには、秘密鍵バックアップ手段11が書きこんだ他のICカードが全て必要になるので、他のICカードがなくなっている場合を考慮して、▲4▼の書きこみ処理を、2重化、3重化してなど、適当な冗長性を持たせるようにしてもよい。

【0019】

上記▲2▼において、ICカード5は、秘密鍵のバックアップコマンドを受けると、分割、暗号化されたデータ61、62、・・・を出力するとしている。これは秘密鍵を分割しつつ暗号化する手段およびその逆処理を行い再構成する手段をICカード5の内部に備えていることを想定している。実施態様としてはこのような態様に限られるわけではない。ICカード5から出力されるのは秘密鍵データそのもので、分割暗号化はパソコン側で、即ち秘密鍵バックアップ手段11が行ってもよい。あるいは、分割と暗号化をICカード5と秘密鍵バックアップ手段11で分担して行ってもよい。いずれの態様でも、秘密鍵の分割データが暗号化されたもの、または、秘密鍵を暗号化したデータを分割したものが得られればよい。

【0020】

【発明の効果】

以上詳しく説明したように、本発明に係る暗号システムを用いれば、秘密鍵、電子証明書を記録したICカードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧するという顕著な効果を奏する。

【図面の簡単な説明】

【図1】本発明に係る暗号システム1の全体構成ブロック図である。

【図2】暗号システム1における秘密鍵のバックアップ動作を説明する図である。

【図3】暗号システム1における秘密鍵のバックアップ動作を説明する図である。

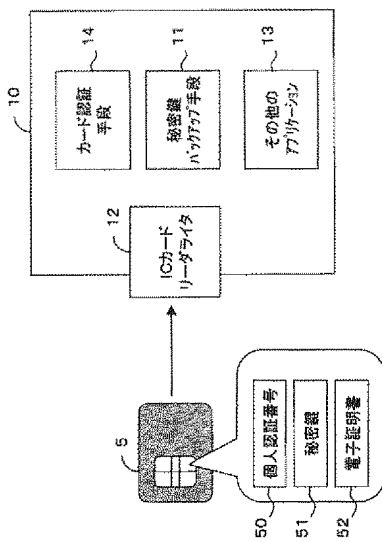
【図4】暗号システム1における秘密鍵の復旧動作の初期段階を説明する図である。

【符号の説明】

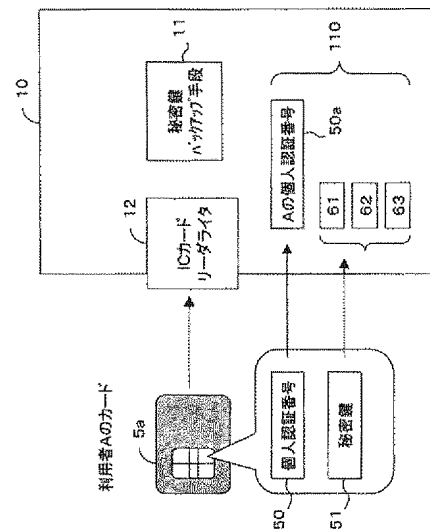
5 ICカード  
10 パソコン  
11 秘密鍵バックアップ手段

- 1 2      I Cカードリーダーライタ
- 1 3      その他のアプリケーション手段
- 1 4      カード認証手段
- 5 0      個人認証番号
- 5 1      秘密鍵
- 6 1      分割暗号化データ
- 6 2      分割暗号化データ
- 6 3      分割暗号化データ
- 1 1 0    バックアップ管理データの集合

【図1】

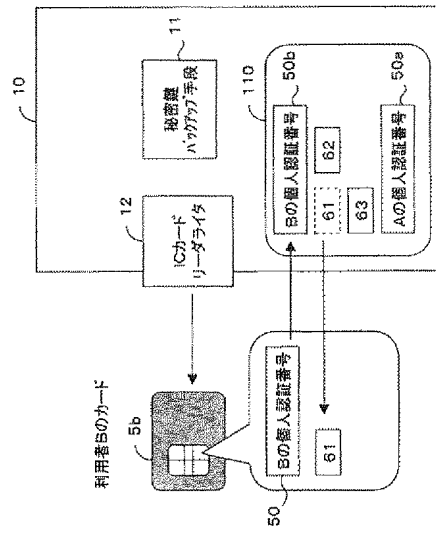


【図2】





【図3】



【図4】

